# Information Governance Policy

| Document Details | | |
|---|---|---|
| **Title** | | Information Governance |
| Main points | | Protecting data processed by the company |
| Who is the document aimed at? | | All staff |
| Author | | |
| **Approval process** | | |
| Approved by (Clinician/Manager) | | EMT |
| Most recent approval date | | October 2024 |
| Category | | General principles |
| Sub Category | | Data and IG |
| Next review date | | October 2025 |
| **Distribution** | | |
| Who the policy will be distributed to | | All staff |
| **Document Links** | | |
| Required by CQC | | |
| Other | | |
| **Amendments History** | | |
| No | Date | Amendment |
| 1 | | |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |

# Background

Dr Laura Neilson is overall Information Governance Lead for the company. Practice Managers have overall responsibility for their practice. Lisa Nolan is the Data Protection Officer for the company.

The key responsibilities of the lead are:-

- To develop an Information Governance Policy with assistance from the NHS E and ICB and /or maintain the currency of the policy;
- To ensure that the practice's approach to information handling is communicated to all staff and made available to the public;
- To work with the DPO to coordinate the activities of staff given data protection, confidentiality, information quality, records management and Freedom of Information responsibilities;
- To work with the Caldicott Lead for the practice ensuring that patient data is kept secure and that all data flows, internal and external are periodically checked against the Caldicott principles;
- To monitor the Practice's information handling activities to ensure compliance with law and guidance;
- To ensure that training made available by the ICB is taken up by staff as necessary to support their role.

The day to day responsibilities for guidance to staff would be undertaken by the practice manager.

# Introduction

This information security policy shall apply to information, systems, networks, applications, locations and staff of Hope Citadel Healthcare. It is based on the expectations set out within the Information Security Management: Code of Practice for NHS organisations.

The purpose of this policy is to enable and maintain effective security and confidentiality of information processed or stored by the practices within Hope Citadel Healthcare. This shall be achieved by:

- Ensuring that all members of staff are aware of and shall comply with relevant legislation, including the GDPR (2016), Data Protection Act (2018) and the Data Protection (Processing of Sensitive Personal Data) Order 2000.
- Ensure all members of staff understand the impact of the Gender Recognition Act 2004
- Describing the principles of information security management and describing how they shall be implemented within Hope Citadel Healthcare
- Introducing an approach to information security that is consistent with other NHS organisations.
- Assisting staff to identify and implement information security as an integral part of their day to day role within the practice.
- Safeguarding information relating to staff and patients under the control of the practice.

## Objectives

Key objectives of this Information Security Policy are to preserve:

- Confidentiality - Access to information shall be restricted to those GPs and staff of each practice and relevant others with agreed authority to view it.
- Integrity – Records are to be complete and accurate with all filing and management systems operating correctly.
- Availability - Information shall be readily available and delivered to the authorised GP or medical professional, when it is needed.

## Responsibilities for Information Security

- Responsibility for information security shall rest with the Caldicott Guardian and the DPO. However, on a day-to-day basis the Practice Manager of each practice shall be responsible for organising, implementing and managing this policy and its related good working practices.
- The Practice Manager shall be responsible for ensuring that both permanent and temporary staff including any contractors and locums are aware of:-
  - The information security policies applicable to their work areas
  - Their personal responsibilities for information security
  - Who to ask or approach for further advice on information security matters.
- All staff shall abide by security procedures as set out by Hope Citadel Healthcare. This shall include the maintenance of Practice records whilst ensuring that their confidentiality and integrity are not breached [this applies to patient, staff and practice information]. Failure to do so may result in disciplinary action.
- This Information Security Policy document shall be owned, maintained, reviewed and updated by Lisa Nolan and the EMT. This review shall take place annually and any results of which shall be made known to the each Practice Manager, who will then pass it on to their staff.
- The staff of each practice shall be responsible for both the security of their immediate working environments and for security of information systems they use (e.g. workstations)
- Any contracts with third party organisations that allow access to the information systems of the practice, shall be in place before access is allowed. These contracts shall ensure that the staff or sub-contractors of those external organisations shall comply with all the appropriate security policies / guidance required by the practice.

1. Contracts of Employment – address information security requirements at the recruitment stage and that all contracts of employment shall contain a confidentiality clause. The information security requirements shall be included within job descriptions.
2. Access Controls - to areas containing information systems are restricted and controlled to ensure that only GPs and those authorised can access information of the Practice.
3. Equipment Security – is effective in order to minimise losses, or damage to the Practice. All information assets and equipment shall, where possible be physically protected from security threats and environmental hazards. (Locked cabinets (fire proof if possible), clear desk policy and the limitation of risks in the surrounding work area etc).
4. Information Risk Assessment – a regular assessment of the working environment, shall be conducted to identify potential risks to the security of Practice information. Where risks are identified, these should be noted and where possible mitigating action taken.
5. Security Incidents and weaknesses - are to be recorded and reported to the Practice Manager and then to the Caldicott Guardian so that they can be investigated to establish their cause, impact and the effect on the Practice and its patients. (NB. remedial changes arising may need to be included within future staff working procedures, updates to policies and contracts of employment).
6. Protection from Malicious Software – should be provided through the use of commercial strength anti-virus/anti-malware software. Where there is an internet connection an appropriate firewall shall be installed and managed. No new software shall be downloaded or installed on computer systems of the Practice without the explicit permission of the Practice Manager, and in some cases the I.T department of the relevant ICB / GM Shared Services. Breach of this requirement may be subject to disciplinary action.

7. Secure Communications – should be in place to ensure that all correspondence, faxes, email, telephone messages and transfer of patient records are conducted in a secure and confidential manner. The communication of NHS Confidential or NHS restricted information by email must be appropriately protected, using cryptographic controls (AES 256 bit or equivalent).
8. Business Continuity and Disaster Recovery Plans – are in place so that in the event of a disruption to the information services of the Practice, it is possible to activate relevant business contingency plans until affected services are restored.

INFORMATION GOVERNANCE POLICY

## 1. Summary

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in clinical governance, service planning and performance management.

It is therefore of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management.

## 2. Principles

Hope Citadel Healthcare recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. Hope Citadel Healthcare fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and commercially sensitive information. Hope Citadel Healthcare also recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest.

Hope Citadel Healthcare believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of everyone in Hope Citadel Healthcare to ensure and promote the quality of information and to actively use information in decision making processes.

There are 4 key interlinked strands to the information governance policy:

- Openness
- Legal compliance
- Information security

- Quality assurance

## 2.1. Openness

- Non-confidential information about Hope Citadel Healthcare and its services should be available to the public through a variety of media, in line with Hope Citadel Healthcare's code of openness
- Hope Citadel Healthcare will establish and maintain policies to ensure compliance with the Freedom of Information Act
- Hope Citadel Healthcare will undertake or commission annual assessments and audits of its policies and arrangements for openness
- Patients should have ready access to information relating to their own health care, their options for treatment and their rights as patients
- Hope Citadel Healthcare will have clear procedures and arrangements for liaison with the press and broadcasting media
- Hope Citadel Healthcare will have clear procedures and arrangements for handling queries from patients and the public

## 2.2. Legal Compliance

- Hope Citadel Healthcare regards all person identifiable information, including that relating to patients as confidential
- Hope Citadel Healthcare will undertake or commission annual assessments and audits of its compliance with legal requirements
- Hope Citadel Healthcare regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise
- Hope Citadel Healthcare will establish and maintain policies to ensure compliance with the Data Protection Act, Human Rights Act and the common law confidentiality
- Hope Citadel Healthcare will establish and maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act)
- Hope Citadel Healthcare will establish and maintain compliance with the Data Protection Act, Human Rights Act and Confidentiality.
- In addition to the Data Protections act 1998 and GDPR 2018, the 2004 GRA deemed a criminal offence to disclose an individual's transgender history to a third party without written consent. Patients do not need to show a GRC or birth certificate. This means always obtaining a trans patients written consent before any relevant information is shared.

## 2.3. Information Security

- Hope Citadel Healthcare will establish and maintain policies for the effective and secure management of its information assets and resources
- Hope Citadel Healthcare will undertake or commission annual assessments and audits of its information and IT security arrangements
- Hope Citadel Healthcare will promote effective confidentiality and security practice to its staff through policies, procedures and training

- Hope Citadel Healthcare will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security

### 2.4. Information Quality Assurance

- Hope Citadel Healthcare will establish and maintain policies and procedures for information quality assurance and the effective management of records
- Hope Citadel Healthcare will undertake or commission annual assessments and audits of its information quality and records management arrangements
- Managers are expected to take ownership of, and seek to improve, the quality of information within their services
- Wherever possible, information quality should be assured at the point of collection
- Hope Citadel Healthcare will promote information quality and effective records management through policies, procedures/user manuals and training

## 3. Responsibilities

The designated Information Governance Lead in each practice is the Practice Manager who responsible for overseeing day to day Information Governance issues; developing and maintaining policies, standards, procedures and guidance, coordinating Information Governance in the practice, raising awareness of Information Governance and ensuring that there is ongoing compliance with the policy and its supporting standards and guidelines.

All staff, whether permanent, temporary or contracted, and contractors are responsible for ensuring that they remain aware of the requirements incumbent upon them for ensuring compliance on a day to day basis.

## 4. Policy Approval

Hope Citadel Healthcare acknowledges that information is a valuable asset, therefore, it is wholly in its interest to ensure that the information it holds, in whatever form, is appropriately governed, protecting the interests of all of its stakeholders.

This policy, and its supporting standards and work instruction, are fully endorsed by the ICB through the production of these documents and their formal approval by Hope Citadel Healthcare.

We will, therefore, ensure that all staff, contractors and other relevant parties observe this policy in order to ensure compliance with Information Governance and contribute to the achievement of the Hope Citadel Healthcare objectives and delivery of effective healthcare to the local population.

*Requirement 10-116*

All staff when they join the practice are asked to sign the companies Staff Confidentiality Agreement. The agreement forms part of their contract with Hope Citadel Healthcare.

In addition, all staff receives a copy of the staff handbook, which goes into more depth of the expectations of staff in regards to Information Governance.

All external staff are required to sign our confidentiality agreement when they begin work with us or have access to areas of the building where they may have access to I.T systems or patient information. These signed agreements are then stored by the Practice Manager. They are valid for one year.

All staff will be routinely monitored in regards to their compliance with the Information Governance and Security policies of Hope Citadel Healthcare.

All incidents, where staff have not complied with the Information Governance and Security policies, will be treated as potential 'gross misconduct' and disciplinary procedure may be started with that member of staff.

*Requirement 10-117*

Each job role with Hope Citadel Healthcare will have an assigned Information Governance and Security training plan which must be completed by all staff. The training plans are determined by which modules are relevant to their job roles. The formal training takes place online and is the official NHS Information Governance training tool.

The Practice Manager of each site is responsible for ensuring that all staff have completed the required training.

Information Governance and Security training is now part of the initial training for all new starters. They will be given basic training during their first two weeks in relation to Hope Citadel Healthcare's policies and procedures.

The formal online training will be required to be completed within the first two months employment with the company. Time will be allocated for this to happen.

Updates to training will be done annually or sooner if the Practice Manager feels the staff member needs additional training. A checklist (appendix 2) of updated training will form part of the staff member's annual appraisal.

Compliance checks and routine monitoring is undertaken to test staff understanding and to ensure procedures are being complied with, where necessary, actions are taken.

*Requirement 10-211*

The areas where personal or sensitive information is sent and/or received within the practice, it must be kept secure and confidential and free from public access.

All staff have a duty to ensure that the unauthorised access to personal or sensitive information in the following areas is maintained.

- Reception Area
- Clinical Rooms
- Admin Office
- Patient Records Storage Room
- Email
- Clinical System
- Printers

Hope Citadel Healthcare follows the Caldicott Principles when transferring patient identifiable information.

| | |
|---|---|
| Principle 1 | Justify the purpose for using confidential information |
| Principle 2 | Only use identifiable information if absolutely necessary |
| Principle 3 | Use the minimum that is required |
| Principle 4 | Access should be on a strict need to know basis |
| Principle 5 | Everyone must understand their responsibilities |
| Principle 6 | Understand and comply with the law |

*Requirement 10-212*

Gaining patient consent is an integral part of patient / health professional relationship. All clinical staff at Hope Citadel Healthcare requests consent from the patient before all procedures, examinations and treatments are commenced. Our consent policy outlines the procedures we have in place gain consent from patients before and treatment or procedure takes place.

*Requirement 10-213*

Due to the nature of what we do, we have access to personal and sensitive information about our patients. It is important that our patients know how we collect information, why we need it and who has access to it.

Information about the personal data we store and the way we collect, store and delete is within our practice leaflet. The practice leaflet is available from our reception desk (and on our website) and is available to all patients.

A poster is also displayed within the reception area highlighting our policy in regards to the handling of our patient's data.

*Requirement 10-304*

All staff who work at one of the Hope Citadel Healthcare practices are given an NHS Smart Card. The smart card enables them to access Choose and Book, issue Electronic Prescriptions and have access to the NHS Demographic Service.

All staff who are issued with a smart card are required to keep the smart card safe and adhere to the national NHS smart card policies and procedures.

Staff should not

- Leave their card in the computer overnight or when they leave for a period of time (e.g. Lunch)
- Let others use their card or give out password

When a member of staff leaves the practice they can either

- Keep their smart card if they are moving to another NHS organisation
- Or hand it to the Practice Manager if they are leaving the NHS

If the staff member hands the card back, the Practice Manager must inform the Registration Authority of this and hand the card to them.

Each Practice Manager will be the site 'Sponsor'

*Requirement 10-316*

An information asset register is compiled at each practice which shows what I.T hardware and software is held at each site. All I.T equipment and software is owned and maintained by our respective ICBs. This asset register is also stored within the Business Continuity Plan.

*Requirement 10-317*

All staff at Hope Citadel Healthcare have a duty to protect our buildings and stored data from being accessed by unauthorised people.

Some examples are

- Locking rooms that are not being used
- Making sure the building is properly secured and alarmed at the end of the day
- Logging off computers when the staff member leaves their desk
- Not leaving patients notes and letters on desks or in view of the public

*Requirement 10-318*

Additional security measures and care must be taken when using mobile devices which store personal information which are taken out of the practice.

Steps must be taken to make sure that only the authorised staff member has access to the device and it is stored securely when not being used.

Currently Hope Citadel Healthcare does not use mobile devices which store patient information.

*Requirement 10-319*

A documented Business Continuity Plan is available at each practice in order to deal with any disruption to core services which may happen unexpectedly.

The plan will show how the plan will be activated, who to contact in emergency, alternative locations in case the practice cannot be used.

The plan is reviewed and tested annually by each practice.

*Requirement 10-320*

All faults and problems with the I.T equipment and software are reported to the I.T department and the respective ICBs.

All information security incidents, near-misses and breaches are reported through the Hope Citadel Healthcare significant event process. This will allow the incident, near-miss or breach to be reported, investigated, learnt from and audited.

Any serious incidents must be reported to the Caldicott Guardian (Dr Rachel Belton) or a member of the EMT if Dr Rachel Belton is not available as soon after the incident as possible.

The associated documents to each requirement can be found at the bottom of this document or within one of the other CQC policies

## Appendix 2

### Staff Training Needs Analysis for Data Security and Confidentiality

All employees need to have annual refresher training on all aspects of Data Security and Confidentiality. This document is designed to act as a guide when training is being planned.